w10

03 August 2021 10:44

mmm... just one more week!

today's topics:
- number theory! (well, basic notions like divisibility and gcd, don't get too excited)
- proof that some number is irrational (guess which proof method we're using!)
- hmm... we're also supposed to review some proofs in the textbook...

Tutorial Worksheet 10

1) Study The Euclidean Algorithm again, and check how proposition 6.2.2 is applied.

try computing gcd(102, 960) using the euclidean algorithm first!

Proposition 6.2.2. Let a, b and k be integers, with a and b not both zero. Then $\gcd(a, b) = \gcd(a - kb, b)$.

the euclidean algorithm is used to compute the gcd of two natural numbers.

$\gcd(15, 25)$
$= \gcd(25, 15)$
$= \gcd(25-15, 15)$
$= \gcd(15, 10)$
$= \gcd(5, 10)$
$= \text{cd}(10, 5)$

$\gcd(102, 960)$
$= \gcd(960, 102)$
$= \gcd(960 - 9 \cdot 102, 102)$
$= \gcd(42, 102)$
$= \gcd(102, 42)$
$= \gcd(102 - 2 \cdot 42, 42)$
$= \gcd(18, 42)$
$= \gcd(42, 18)$
$= \gcd(42 - 2 \cdot 18, 18)$
$= \gcd(6, 18)$
$= \gcd(18, 6)$
$= \gcd(18 - 3 \cdot 6, 6)$
$= \gcd(0, 6) = 6.$

3) Let $a, b \in \mathbb{N}$ and $d = gcd(a, b)$. Prove that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

(you can just show that a/d, b/d don't have any positive factors in common besides 1)

Pf #1 we show $\frac{a}{d}, \frac{b}{d}$ don't have any divisors > 1.

Let $k > 1, k \in \mathbb{N}$. Suppose (towards a contradiction) $k \mid \frac{a}{d}$ and $k \mid \frac{b}{d}$.

Since $k \mid \frac{a}{d}$, $mk = \frac{a}{d}$ for some $m \in \mathbb{Z}$.

$\Rightarrow mdk = a$

so dk divides a.

similarly, dk divides b.

so dk divides both a and b,

but $dk > d = \gcd(a, b)$

since $k \geq 2$

so d isn't the greatest common divisor. $\Rightarrow\Leftarrow$

Pf #2

Theorem 6.2.4. *(Bézout's Identity)*

Let a and b be two integers, not both zero. Then there are $m, n \in \mathbb{Z}$, such that

$$a \cdot m + b \cdot n = \gcd(a, b).$$

Let $m, n \in \mathbb{Z}$ s.t. $am + bn = d$

$$\Rightarrow \left(\frac{a}{d}\right)m + \left(\frac{b}{d}\right)n = 1$$

if $k \in \mathbb{Z}$, $k > 1$, and $k \mid \frac{a}{d}$ and $k \mid \frac{b}{d}$

then $k \mid 1$. but $k > 1$??

2) Study the uniqueness part of the fundamental theorem of arithmetics again.

Theorem 6.3.3 (The Fundamental Theorem of Arithmetic)**.** *Every natural number $n \geq 2$ is either a prime, or can be expressed as a product of powers of distinct primes, in a unique way (except for reordering of the factors).*

Proof. We have already proved the existence part of the theorem (Theorem 4.5.1). We thus proceed by proving **the uniqueness part**, using strong induction.

For the base case, $n = 2$, the theorem holds true, as 2 is a prime number. Assume that the uniqueness part of the theorem is true for $n = 2, 3, 4, \ldots, k$, and consider the number $k + 1$. We already know that $k + 1$ is a prime number, or can be expressed as a product of prime numbers. Our task is to prove that, if $k + 1$ is composite, then its factorization is unique.

We use a similar strategy we used in the proof of the Division Algorithm (Theorem 6.1.2). Suppose that we can factor $k + 1$, as a product of distinct powers of primes, in two ways. That is

$$k + 1 = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_\ell^{a_\ell} \;=\; q_1^{b_1} \cdot q_2^{b_2} \cdot \cdots \cdot q_m^{b_m}\,, \qquad (*)$$

where $p_1, \ldots, p_\ell, q_1, \ldots, q_m$ are prime numbers, and $a_1, \ldots, a_\ell, b_1, \ldots, b_m$ are natural numbers.

Clearly, $p_1 | k + 1$, as p_1 appears in the product $p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_\ell^{a_\ell}$. Therefore, p_1 must divide the other representation of $k + 1$:

$$p_1 | q_1^{b_1} \cdot q_2^{b_2} \cdot \cdots \cdot q_m^{b_m}.$$

Now, as p_1 is prime, we conclude, from Euclid's Lemma, that it must divide one of the numbers $q_1, \ldots, q_m$. Assume, for simplicity, that $p_1 | q_1$ (if p_1 divides one of the other q's, we can re-assign indices, so that $p_1 | q_1$).

Remember that q_1 is also a prime number, and so its only positive divisors are 1 and q_1. As $p_1 \neq 1$, we conclude that $p_1 = q_1$. We now divide the equalities $(*)$ by p_1 (or, equivalently, by q_1), and obtain

$$\frac{k+1}{p_1} = p_1^{a_1 - 1} \cdot p_2^{a_2} \cdot \cdots \cdot p_\ell^{a_\ell} \;=\; q_1^{b_1 - 1} \cdot q_2^{b_2} \cdot \cdots \cdot q_m^{b_m}\,.$$

Finally, we can use the induction hypothesis to complete the proof. As $\frac{k+1}{p_1}$ is smaller than $k + 1$, it is covered by our hypothesis, and thus satisfies the uniqueness part of the theorem. This means that the p's, the q's, and the corresponding exponents must be the same. More explicitly,

- The number of factors is the same. That is, $\ell = m$.
- The prime factors themselves have to be the same, though perhaps in some other arrangement. Thus, possibly after some re-indexing, we have $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_\ell = q_\ell$.
- The exponents on the factors have to be the same, i.e., $a_1 - 1 = b_1 - 1$, $a_2 = b_2$, $\ldots$, $a_\ell = b_\ell$.

We conclude, from the above observations, that the two initial factorizations for $k+1$ (in $(*)$) were identical, as needed. We have thus proved the uniqueness part for $k+1$, which concludes the proof of the theorem. □

4) Prove that $\sqrt[3]{20}$ is an irrational number.

(see claim 6.3.2 if you need a hint on how to proceed)

Claim 6.3.2. The number $\sqrt{7}$ is irrational. That is, $\sqrt{7} \notin \mathbb{Q}$.

Proof. We prove the claim by contradiction. Assume that $\sqrt{7}$ is a rational number. Then $\sqrt{7} = \frac{a}{b}$ for some nonzero integers a, b. As $\sqrt{7} > 0$, we may assume that $a, b > 0$. Moreover, we assume that $\gcd(a, b) = 1$ (namely, a and b are relatively prime), in which case the fraction $\frac{a}{b}$ is said to be in **lowest terms**, or **completely reduced**.

From the equality $\sqrt{7} = \frac{a}{b}$, we get

$$7 = \frac{a^2}{b^2} \quad \Rightarrow \quad 7b^2 = a^2,$$

and hence $7|a^2$ (or $7|a \cdot a$). By Euclid's Lemma, $7|a$, and hence $a = 7n$ for some integer n. Replacing a by $7n$ gives

$$7b^2 = (7n)^2 \quad \Rightarrow \quad 7b^2 = 49n^2 \quad \Rightarrow \quad b^2 = 7n^2,$$

from which we conclude that $7|b^2$. Again, by Euclid's Lemma, we see that $7|b$, leading to a contradiction. The fraction $\frac{a}{b}$ was assumed to be in lowest terms, which is inconsistent with our conclusion, that both a and b are divisible by 7.

Consequently, our initial assumption must be false, and thus $\sqrt{7} \notin \mathbb{Q}$. $\square$

Pf Assume (for contradiction)

$\sqrt[3]{20} = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$.

we may also assume $\gcd(p,q) = 1$

$\sqrt[3]{20} = \frac{p}{q} \Rightarrow 20 = \frac{p^3}{q^3} \Rightarrow 20q^3 = p^3$

$2 | 20q^3$ so $2 | p^3$

so $2 | p \cdot p \cdot p$

Claim 6.3.1 (Euclid's Lemma[2]).
Let $p > 1$ be a prime number, and $a, b \in \mathbb{Z}$. If $p|ab$, then $p|a$ or $p|b$.

so $2 | p$.

write $p = 2m$ for some $m \in \mathbb{Z}$.

$20q^3 = p^3$

$\Rightarrow 20q^3 = (2m)^3 = 8m^3$

$\Rightarrow 5q^3 = 2m^3$

$2 | 2m^3$ so $2 | 5q^3$

so $2 | 5 \cdot q \cdot q \cdot q$

by Euclid's lemma, since $2 \nmid 5$, it must be true that $2 | q$.

so $2|p$ and $2|q$, but $\gcd(p,q) = 1$. $\Rightarrow \Leftarrow$